REMARKS

Applicants respectfully traverse the rejections of the pending claims. In particular, claim 36 has been amended to point out the following feature of Applicants' invention. Before discussing this feature, Applicants submit that it would be helpful to review the revocation scheme disclosed in the Nonaka publication (2003/0046238). As discussed with regard Figure 1 in ¶179, a user home network 103 includes a "network device" 160_1 (which will be referred to hereinafter as the "network device SAM") and audio-visual machines 160_2 through 160_4. All of these networked devices include a "secure application module" (SAM) (the audio-visual machines will be referred to hereinafter as the "audio-visual SAMs"). The network device receives a "secure container" file 104 from a content provider 101. To gain access to the encrypted content within the secure container, the network device interfaces with an "EMD service center" 102. The secure container may be received over the Internet or may be received offline in a storage medium as shown in Figures 11 – 16.

Nonaka describes no revocation whatsoever between the network device and the content provider. Moreover, note that even if Nonaka did describe revocation in this context (although he did not), such revocation would be with regard to the entire secure container and not to specific files within the secure container. Instead, as described in ¶671, revocation is between the SAMs. Specifically, "in performing communication between the SAMs, each SAM checks the revocation list for whether the corresponding SAM has become invalid, in which case, the communication therebetween is discontinued." Although Nonaka never explicitly addresses the issue, it is evident that this revocation check occurs during the "mutual authentication" of the corresponding

SAMs as discussed, for example, in ¶516, which concerns the playback of content in one of the audio/visual SAMs as governed by the network device SAM.

Given this context, the amendment to claim 36 will now be addressed. In general, it is known in digital rights management (DRM) to use certificates that are presented between devices to establish authenticity. Because there is the possibility of a device obtaining a valid certificate through improper means, DRM schemes often provide for a revocation step following authentication of the certificate. In other words, a device may present a valid certificate but may be revoked because of its improper actions. Thus, DRM schemes often include the step of checking a device's identity subsequent to authentication of a valid certificate against a revocation list. If the device is indicated as revoked, access is cut off despite the possession of a valid certificate.

Once a device has been established as authentic and not revoked, conventional DRM schemes may proceed to respond to file requests, etc. However, Applicants' DRM scheme is different. As set forth, for example, on page 30, line 3 through page 35, line 21 with regard to Figures 7A-7F, Applicants granular, file-by-file revocation scheme proceeds subsequent to establishment of a secure session. As shown in Figures 7A and 7B, a host presents a certificate to the storage engine. If the certificate is authentic, the storage engine transmits a secure session key to the host to establish a secure session. During this secure session, various file requests may be issued by the host as discussed with regard to Figures 7C-7F. This file requests are checked on a file-by-file basis. Thus, a host may be revoked with regard to a first file but not with regard to a second file. Such revocation flexibility is unavailable in conventional DRM schemes.

Claim 36 reflects this advantageous flexibility in that it requires that the acts of "receiving at the storage engine a file request from the host device, the file request being directed to a file stored on a storage medium accessible to the storage engine; reading a revocation file associated with the file from the storage medium, the revocation file containing at least one rule, the at least one rule associating data in the revocation file with data in the certificate; applying the at least one rule on the data in the revocation file and the associated data in the certificate; and if the application of the at least one rule provides a failing result, denying the file request" are performed subsequent to the establishment of a secure session as required by the added limitation of "establishing a secure session by transmitting a session key to the host device; and during the secure session:" No new matter is added, the support being as discussed above.

Thus, revocation is a file-by-file decision during the secure session recited in claim 36. A host may be authenticated and be allowed to read a given file during a secure session but not another. Given this context, it becomes clear that the SAMs in Nonaka do not represent a "host device" and a "storage engine" as recited in claim 36. Specifically, Nonaka never teaches or suggests the following: subsequent to authentication and establishment of a secure session, responding to a file request by checking for revocation as recited in claim 36. Instead, the Nonaka revocation (to the extent that this revocation is disclosed) is simply the all-or-nothing revocation of the prior art. In particular, note that the file request (the internal interrupt to play content as set forth in ¶514) occurs first. Subsequent to this request, there is mutual authentication and exchange of a session key as set forth in ¶516. Thus, Nonaka is entirely "upside down" with regard to claim 36, which requires the authentication and secure session to be established first. Moreover, Nonaka makes absolutely no teaching or suggestion for the recited acts of "reading a revocation file associated with the file from the storage medium, the revocation file containing at least one rule, the at least one rule associating data in the revocation file with data in the certificate; [and] applying the at least one rule on the data in the revocation file and the associated data in the certificate." Instead, all Nonaka does is check a revocation list, which lists identities of revoked devices.

Accordingly, the pending claims are allowable over the Nonaka publication.

Claims 42 and 43 are cancelled.

Applicant respectfully traverses the assertion that the rule recited in claim 36 is suggested by Nonaka's teaching "the number of times of content play or effective period for play/copy as taught in Nonaka." Instead, Nonaka's play privileges and related permissions are controlled by the usage log data 108 and UCS data 166 sent by the network device SAM to the EMD service center 102 as seen in Figure 1. Such a teaching is irrelevant to the method of claim 36, which provides a file-by-file revocation scheme as discussed above.

CONCLUSION

For the above reasons, pending Claims 36-40 are in condition for allowance and allowance of the application is hereby solicited. If the Examiner has any questions or concerns, a telephone call to the undersigned at (949) 752-7040 is welcomed and encouraged.

Certification of Facsimile Transmission

I hereby certify that this paper is being facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Jonathan Hallman

May 15, 2006
Date of Signature

Respectfully submitted,

Jonathan W. Hallman
Attorney for Applicants
Reg. No. 42,622